IMPLEMENTASI STEGANOGRAPHY PADA AUDIO MENGGUNAKAN ALGORITMA END OF FILE (EOF)

Angga Aditya Permana[1]

Prodi Teknik Informatika, Fakultas Teknik, Universitas Muhammadiyah Tangerang

Jl. Perintis Kemerdekaan I/3.
email: anggaumt@gmail.com

Abstract - Steganography is the art and science of writing hidden messages or hiding messages in a way so that apart from the sender and the recipient no one knows or is aware that there is a secret message. The message is hidden into a media that is audio. One of the methods used in hiding information into audio is the End of File (EOF) method. The purpose of this study is to implement the EOF method to insert messages into audio files. The EOF method works by adding message decimal values to audio files.

Keyword : Steganography, Audio, Eond Of File

Abstrak - Steganografi merupakan seni dan ilmu menulis pesan tersembunyi atau menyembunyikan pesan dengan suatu cara sehingga selain si pengirim dan si penerima tidak ada seorangpun yang mengetahui atau menyadari bahwa ada suatu pesan rahasia. Pesan tersebut disembunyikan kedalam sebuah media yaitu audio. Metode yang digunakan dalam menyembunyikan informasi kedalam audio salah satunya menggunakan metode End Of File (EOF). Tujuan penelitian ini untuk mengimplementasikan metode EOF untuk menyisipkan pesan kedalam file audio. Metode EOF bekerja dengan menambahkan nilai desimal pesan ke dalam file audio.

Kata Kunci : Steganografi; Audio; EOF

I. PENDAHULUAN

Perkembangan media digital sangat pesat dengan maraknya penggunaan teknologi informasi serta transfer data dari pihak pengirim ke pihak penerima dan semakin banyak menimbulkan keresahan dalam mengirim suatu informasi. Salah satu teknik dalam mengirimkan dan mengamankan informasi menggunakan metode Steganografi. Steganografi merupakan seni dan ilmu menulis pesan tersembunyi atau menyembunyikan pesan dengan suatu cara sehingga selain si pengirim dan penerima tidak ada seorang pun yang mengetahui atau menyadari bahwa ada pesan rahasia.Permana (2017). Steganografi memiliki beberapa metode salah satunya merupakan metode *End Of File* (EOF). Metode *End Of File* (EOF) memiliki keunggulan karena cara kerjanya, yaitu dengan menyisipkan pesan rahasia pada akhir file *covernya* sehingga pesan rahasia yang yang ingin dilindungi dapat disisipkan dalam jumlah yang tidak terbatas. Media yang digunakan dalam metode ini juga bermacam-macam seperti teks, gambar, audio atau video, dan pesan yang disembunyikan bisa berbagai macam tipe data, bisa berupa text, gambar audio ataupun video. Permana (2017) telah melaporkan metode steganografi yang diaplikasikan untuk pengamanan teks pada gambar dengan algoritma *blowfish* dan *Least Significant Bit*. Pengamanan data dilakukan dalam bentuk teks dengan *cover* berbentuk gambar, Data lain selain dari teks juga perlu diamankan, dan *covernya* dalam hal ini ialah audio. Pada penelitian ini menggunakan media audio sebagai file *cover* untuk menyisipkan pesan yang ingin disembunyikan.

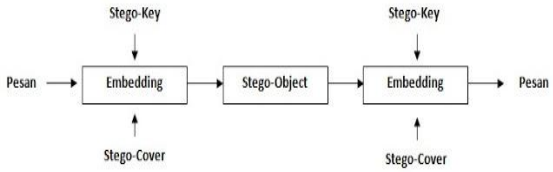
II. KAJIAN LITERATUR

Steganography

Steganografi memanfaatkan media digital untuk menyisipkan pesan rahasia melalui kode biner pada media digital tersebut, seperti: gambar, audio, video, text atau file biner. Wibowo (2017).

Steganography merupakan seni dan ilmu menulis dan menyembunyikan pesan rahasia dengan suatu cara sehingga selain si pengirim dan penerima tidak ada seorang pun yang mengetahui atau menyadari bahwa ada suatu pesan rahasia di dalamnya. Permana (2017) Steganography sendiri telah digunakan 2.500 tahun yang lalu untuk kepentingan politik, militer, diplomatik serta kepentingan pribadi sebagai alat. Teknik dalam menyembunyikan pesan sebenarnya ada dua yaitu Steganography dan Kriptography. Perbedaan nya adalah Kriptografi menjaga pesan dengan cara mengubah bentuk pesan agar tidak dapat dipahami oleh orang lain.

Firmansyah dan Permana (2019) Sementara Steganography menyembunyikan pesan dalam sebuah medium seperti gambar, video maupun audio. Salah satu keuntungan steganography di bandingkan dengan kripftography adalah bahwa pesan yang dikirim tidak menarik perhatian sehingga media penampung pesan tidak menimbulkan kecurigaan bagi pihak ketiga.



Gambar 1. Proses Steganografi

Secara umum, terdapat dua proses *steganography* yaitu *embedding* untuk menyisipkan pesan ke dalam *cover object* dan proses decoding untuk ekstraksi pesan dari *stego-object*. Kedua proses ini mungkin memerlukan kunci rahasia yang dinamakan *stego key* agar pihak yang berhak saja yang dapat melakukan penyisipan dan ekstraksi pesan.

Menurut alatas (2009) Dalam penyembunyian pesan rahasia kedalam media digital memiliki kriteria yang harus di perhatikan yaitu :

- *Fidelity*

Mutu citra penampung tidak jauh berubah setelah penambahan pesan rahasia sehingga hasil steganography masih terlihat dengan baik.

- *Robustness*

Data yang disembunyikan harus tahan terhadap manipulasi yang dilakukan pada citra penampung.

- *Recovery*

Data yang disembunyikan harus dapat diungkap kembali karena tujuan steganography adalah data hiding maka sewaktu-waktu pesan rahasia di dalam citra penampung harus dapat diambil kembali untuk digunakan lebih lanjut.

Menurut pendapat Arius (2006) bahwa tujuan dari steganografi ini adalah merahasiakan atau menyembunyikan keberadaan dari sebuah pesan tersembunyi atau sebuah informasi.

Steganography memiliki tujuh jenis teknik yaitu :

- *Injection*

Merupakan suatu teknik menanamkan pesan rahasia secara langsung ke suatu media.

- *Substitusi*

Data normal digantikan dengan data rahasia. Biasanya hasil teknik ini tidak terlalu mengubah ukuran data asli tetapi tergantung pada file media dan data yang akan disembunyikan.

- *Transformasi Domain*

Merupakan teknik menyembunyikam data pada transform space.

- *Spread Spectrum*

Merupakan teknik pentransmisisan menggunakan pseudo-noise code

- *Statistical Method*

Menanamkan satu bit informasi pada media tumpangan dan mengubah statistic walaupun hanya 1 bit.

- *Distortion*

Metode ini menciptakan perubahan atas benda yang ditumpangi oleh data rahasia.

- *Cover Generation*

Ini lebih unik daripada metode lainnya karena cover object dipilih untuk menyembunyikan pesan.

Menurut Rinaldi, 2006, terdapat beberapa istilah yang berkaitan dengan steganografi yaitu :

1. Carrier file : file yang berisi pesan rahasia tersebut.
2. Steganalysis : proses untuk mendeteksi keberadaan pesan rahasia dalam suatu file.
3. Stego-medium : media yang digunakan untuk membawa pesan rahasia.
4. Redundant bits : sebagian informasi yang terdapat di dalam file yang jika dihilangkan tidak akan menimbulkan kerusakan yang signifikan (setidaknya indera manusia).
5. Payload : informasi yang akan disembunyikan

***End Of File* (EOF)**

Metode *End Of File* merupakan salah satu metode yang digunakan dalam steganography. Metode ini menggunakan cara dengan menyisipkan data pada akhir file. Teknik ini dapat digunakan untuk menyisipkan data yang ukurannya sama dengan ukuran file asli ditambah dengan ukuran data yang akan disisipkan kedalam file tersebut. Dalam teknik End Of File data yang disisipkan pada akhir diberi tanda khusus sebagai pengenal start dari data tersebut dan pengenal akhir dari data tersebut. Anggraini dan Sakti (2014)

Menurut Wandani (2012), tahapan proses embedding atau penyisipan pesan menggunakan metode End of File adalah sebagai berikut : 1). Inputkan ciphertext yang akan disisipkan. 2). Inputkan citra yang akan menjadi media penyisipan ciphertext (cover image). 3). Baca nilai setiap pixel citra. 4). Baca nilai setiap pixel citra. 5). Petakan menjadi citra baru.

Dalam metode *End Of File* pesan yang akan disisipkan pada media akan di konvert kedalam nilai desimal berdasarkan tabel ASCII. Kode ASCII merupakan representasi numerik dari karakter-karakter yang digunakan pada computer, dengan ketentuan huruf a-z, A-Z, 0-9 dan symbol standar pada keyboard. Keunggulan metode End Of File dibandingkan dengan metode yang lain adalah karena disisipkan pada akhir file, pesan yang disisipkan tidak bersinggungan dengan isi file, hal ini menyebabkan integritas data dari file yang disisipi tetap dapat terjaga. Namun metode ini memiliki kelemahan yaitu mengubah besar ukuran file namun tidak mengubah format file dari media yang dipakai sebagai tempat penyisipam pesan tersebut.

Audio Digital

Audio digital merupakan versi digital dari suara analog. Pengubahan suara analog menjadi suara digital membutuhkan suatu alat yang disebut analog to digital converter (ADC). ADC akan mengubah amplitude gelombang sebuah analog menjadi digital yang merupakan proses konversi. Audio digital adalah harmonisasi bunyi yang dibuat melalui perekaman konvensional maupun suara sintetis yang disimpan dalam media berbasis teknologi computer. Format encoding digital dapat menyimpan data dalam jumlah besar, jangka panjang dan berjaringan luas. Sebagai proses digitalisasi terhadap format rekaman music analog, lagu atau music digital mempunyai beraneka ragam format yang bergantung pada teknologi yang digunakan. Contoh formatnya seperti MP3, WAV, AAC, WMA, Ogg dan lain-lain. Binanto (2010)

Berkaitan dengan audio digital adalah istilah Codec audio yang memiliki dua arti encode (mengkodekan) dan decode (menguraikan kode). Codec adalah nama teknis yang diambil dari singkatan compression/decompression atau juga coder/decoder yang artinya adalah program computer yang berfungsi mengecilkan (compress) file-file lalu dikembalikan ke ukuran semula (decompress). File-file multimedia seperti audio, mp3 atau lagu dan file-file film atau video biasanya punya ukuran besar, disinilah codec dibutuhkan.

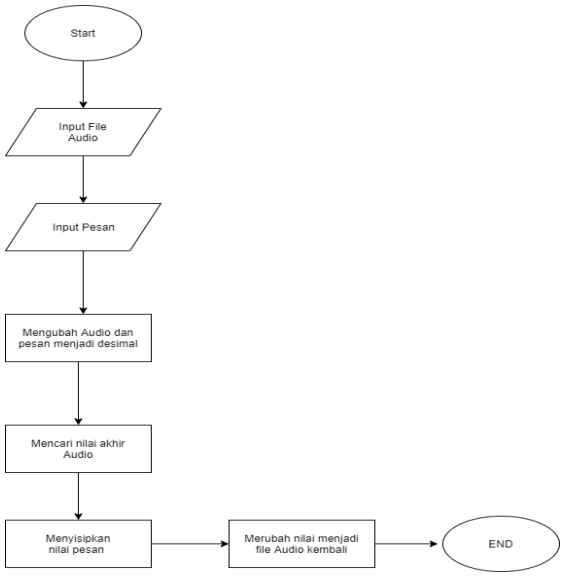
Pada perangkat lunak, codec adalah program computer yang menempatkan data digital audio sesuai format file audio yang diberikan.

Cara untuk mengaplikasikan steganography pada file audio terdiri dari beberapa cara yang lazim digunakan dan prinsip kerja atau algoritma yang digunakan sama seperti pada metode steganography pada gambar. Audio digital berbeda dari suara analog tradisional dimana ini adalah sinyal diskrit dan bukan sinyal kontinu. Sinyal diskrit diciptakan dari sampling sinyal analog yang kontinu dengan rate tertentu. Sebagai contoh, sampling rate pada CD audio digital pada umumnya adalah 44 KHz (artinya dalam 1 detik ada sekitar 44000 sampel yang dimaninkan) Gambar berikut menggambarkan gelombang suara analog (kontinu) yang mengalami sampling untuk menghasilkan audio digital. Aksani dan Manurung (2017)

Flowchart

Proses Penyisipan Pesan

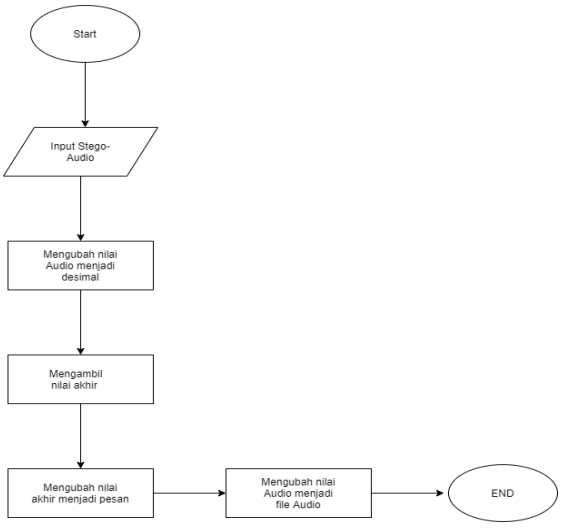
Langkah-langkah proses penyisipan pesan rahasia ke dalam audio menggunakan metode end of file adalah sebagai berikut :



Gambar 2. Flowchart penyisipan pesan

Proses Ekstraksi Pesan

Langkah-langkah proses ekstraksi pesan yang berada dalam stego-audio menggunakan metode end of file :

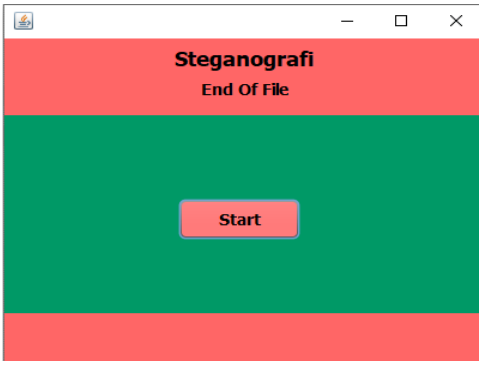


Gambar 3. Flowchart ekstraksi pesan

III. HASIL DAN PEMBAHASAN

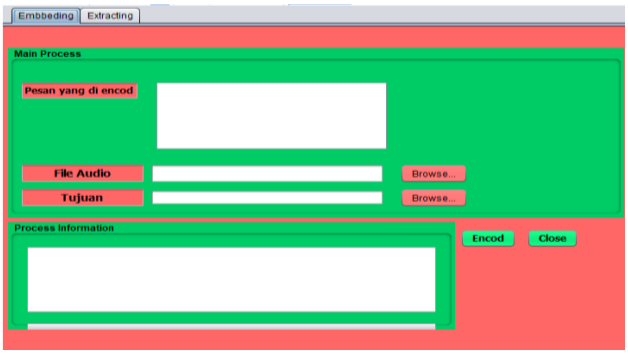
Tampilan Aplikasi

Menu utama untuk memulai program *embedding* dan *extracting*.



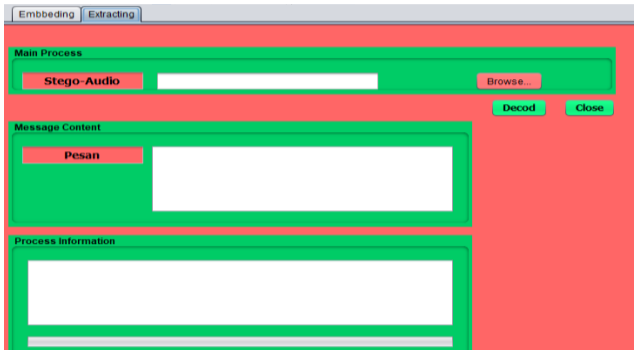
Gambar 4. Menu Utama

Menu *embedding* untuk melakukan proses *encod*. Terdapat *field* pesan yang akan di *encod*, file audio dan tujuan yang harus diisi.



Gambar 5. Menu Embedding

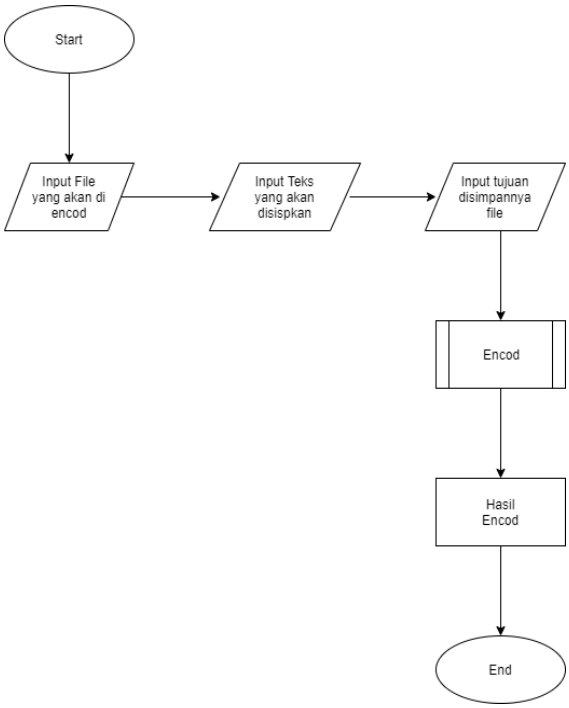
Menu *extracting* untuk melakukan proses decod. Didalam nya terdapat field stego audio yang harus diisi dan field pesan untuk menampilkan isi pesan yang disembunyikan serta field informasi proses.



Gambar 6. Menu Extracting

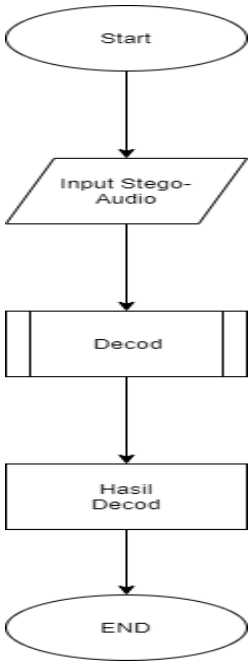
Flowchart Aplikasi

Flowchart Aplikasi Encode



Gambar 7. Flowchart Encode

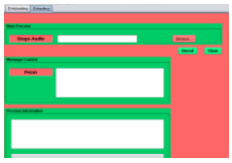
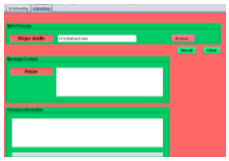
Flowchart Aplikasi Decode



Gambar 8. Flowchart Aplikasi Decode

PENGUJIAN

Tabel 1. Pengujian BlackBox

NO	Skenario Pengujian	Hasil yang Diharapkan	Kesimpulan
1.	Mengosongkan field untuk mencantumkan audio dan teks Test Case : 	Sistem akan menolak proses encode dan menampilkan pesan "Tidak ada file audio yang dipilih" Hasil Pengujian : 	Valid
2.	Mengisi field pesan dan audio tetapi mengosongkan field tujuan Test Case : 	Sistem akan menolak proses encode dan menampilkan pesan "Tidak ada tujuan yang dipilih" Hasil pengujian : 	Valid
3.	Mengisi field pesan, audio dan tujuan untuk proses encode Test Case : 	Sistem menerima proses encode dengan menampilkan informasi proses dan file tersimpan ke tujuan. Hasil Pengujian : 	Valid
4.	Mengosongkan field stego audio untuk melakukan proses decod. Test Case : 	Sistem tidak dapat melakukan proses decod dan menampilkan pesan "Tidak ada file yang dipilih". Hasil Pengujian : 	Valid
5.	Mengisi field stego audio untuk melakukan proses decod. Test Case : 	Sistem akan melakukan proses decod dengan menampilkan informasi proses dan isi pesan yang di sembunyikan. Hasil Pengujian : 	Valid

IV. KESIMPULAN

Berdasarkan aplikasi yang telah dibuat yaitu program Steganografi End Of File untuk mengamankan pesan rahasia kedalam audio. Dapat disimpulkan bahwa metode ini memproses data dengan cara mengubah menjadi bilangan desimal dan disisipkan diakhir file audio. Teknik ini tidak membuat kecurigaan pada file yang disisipi pesan karena tidak merubah audio. Kekurangan dari metode ini adalah adanya sedikit perubahan dalam ukuran file.

V. DAFTAR PUSTAKA

[1.] Aksani, M, L dan Manurung, I, F, (2017), Studi Dan Implementasi Steganografi Pada Citra JPEG Dengan Metode Spread Spectrum, JIKA (Jurnal Informatika), Vol 1 No 2, ISSN : 2549-0710.

[2.] Alatas, P., 2009. Implementasi Teknik Steganografi Dengan Metode LSB Pada Citra Digital. Jakarta: Universitas Gunadarma

[3.] Anggraini. Y dan D. V. S. Y. Sakti (2014), Penerapan Steganografi Metode End of File (Eof) Dan Enkripsi Metode Data Encryption Standard (Des) Pada Aplikasi Pengamanan Data Gambar Berbasis Java, Konf. Nas. Sist. Informasi, STMIK Dipanegara Makassar, ISSN : 1743–1753.

[4.] Arius, D., (2006). Computer Security. Yogyakarta: ANDI

[5.] Binanto, I (2010), Multimedia Digital - Dasar Teori dan pengembangannya, Yogyakarta : penerbit andi, isbn : 978 - 979 - 29 - 1328 – 6.

[6.] Firmansyah, R dan Permana, A, A,. 2019, Implementasi Keamanan Pesan Teks Menggunakan Kriptografi Algoritma RSA dengan Metode Waterfall berbasis JAVA, Joutica Vol 4 No 1, ISSN : 2621-511X.

[7.] Permana, A, A. 2017. Aplikasi penyisipan teks pada gambar dengan algoritma blowfish dan least significant bit. JIKA (Jurnal Informatika), Vol 1 No 1, ISSN : 2549-0710.

[8.] Rinaldi M,(2006) “KRIPTO Informatika, Hal 304.

[9.] Wandani, H.; Budiman, M.A; Sharif, A., (2012). Implementasi Sistem Keamanan Data dengan Menggunakan Teknik Steganografi End of File (EOF) dan Rabin Public Key Cryptosystem. Jurnal Alkhawarizimi, 1 (1).

[10.] Wibowo, A. 2017, Prototype "Pengamanan Ganda" pesan rahasia dengan menggunakan teknik Steganografi metode LSB dan Kriptografi metode Vigenere Cipher. JIKA (Jurnal Informatika), Vol 1 No 2, ISSN : 2549-0710.